Integral AES 256 Bit Crypto SSD Underlying PCB

Integral Memory PLC.

FIPS 140-2 non-Proprietary Security Policy

Module Document Version: 1.5

Table of Contents

Table of Figures

Table of Tables

1. Introduction

1.1. Purpose

This is a non-proprietary FIPS 140-2 Security Policy for the Integral AES 256 Bit Crypto SSD Underlying PCB Cryptographic Modules. It describes how these modules meet all requirements as specified for FIPS 140-2, Security Level 2. This policy forms a part of the submission package to the security testing (CST) Laboratory.

FIPS 140-2 (Federal Information Processing Standard Publication, 140-2) specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the standard, visit:

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

1.2. References

This Security Policy describes how this module complies with the eleven sections of FIPS 140-2:

- For more information on the FIPS 140-2 standard and CMVP please refer to the NIST website at http://csrc.nist.gov/groups/STM/cmvp/index.html

- For more information about Integral Memory Solutions please visit www.integralmemory.com/crypto/

1.3. Document History

Author(s)	Version	Date	Comment
Patrick Warley	1.0	05/29/2013	FIPS Submission Draft
Patrick Warley	1.1	10/06/2015	FIPS Submission Draft
Patrick Warley	1.2	02/18/2015	FIPS Submission Draft
Patrick Warley	1.3	02/22/2016	FIPS Submission Draft
Patrick Warley	1.4	03/15/2016	FIPS Submission Draft
Patrick Warley	1.5	06/05/2017	FIPS Submission Draft

2. Cryptographic Module Description

2.1. The Integral AES 256 Bit Crypto SSD Underlying PCB

The Integral AES 256 Bit Crypto SSD Underlying PCB is an internal storage device which has mandatory encryption for all data including the operating system. The Integral 256 Bit Crypto SSD Underlying PCB comes in 32 GB, 64 GB, 128 GB, 256 GB, 512 GB, 1 TB and 2 TB versions. The devices feature many security enhancements including an epoxy resin coating around both the circuit components and the printed circuit board (PCB). The module implements AES, XTS, in FIPS Approved Mode.

The devices require an operating system to be installed to operate the encryption program which must be in a desktop or laptop computer with Microsoft Windows® operating system. The encryption program SSDLock can be run from the Desktop or from the USB Drive that is supplied with the Crypto SSD. With this you will be able to run a software package (called SSDLock) directly. The software GUI has a people friendly interface that makes using the drive simple and easy but does not compromise security.

The encryption is carried out using AES (256 bit in XTS and CBC mode & AES 128 bit in XTS Mode). It also supports identity based authentication with a strong user password of at least 8 and a maximum of 16 characters. The password must contain both upper and lower case letters, and include at least one numeric and special character. For further protection the Integral 256 Bit Crypto SSD allows a maximum of 20 incorrect password attempts in user or Admin Mode before destroying all data on the device. This protects against brute force attacks on the drive.

The Integral 256 Bit Crypto SSD Underlying PCB has a Multi-Lingual interface in 13 languages.

2.2. Cryptographic Module Specification

The modules are multi-chip standalone cryptographic modules as defined by FIPS PUB 140-2, and meet the overall requirements applicable to Level 2. The cryptographic boundary for the modules (demonstrated by the red line in ***Figure 1***) is defined as the steel chassis which contains all integrated circuits. All components of the module are production grade and the module is opaque within the visible spectrum. The modules execute proprietary non-modifiable S5FDM018 firmware.

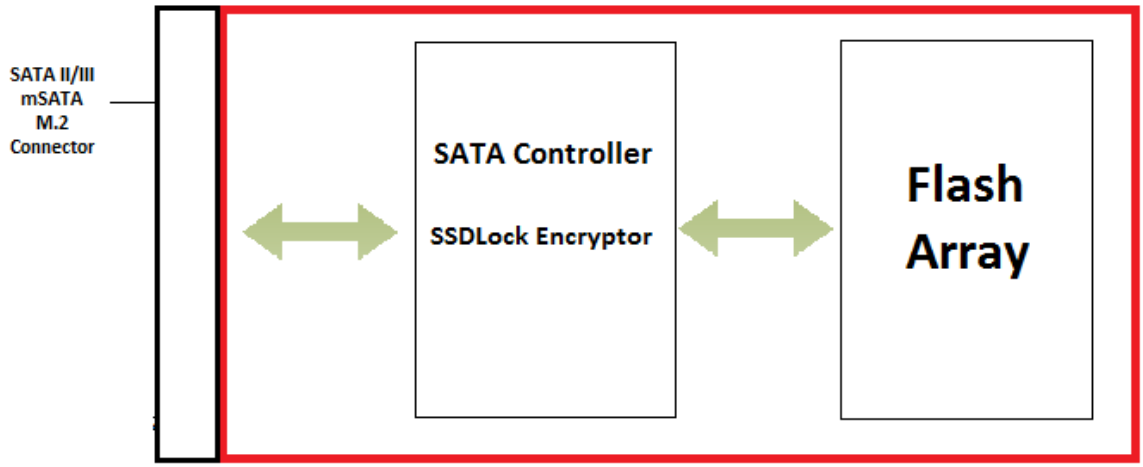

Figure 1 – Cryptographic Module Block Diagram

2.3. Module Compliance to FIPS 140-2 Sections

The Integral AES 256 Bit Crypto SSD Underlying PCB modules conform to the following Sections of FIPS 140-2:

Section	***Level***
1. Cryptographic Module Specification	2
2. Cryptographic Module Ports and Interfaces	2
3. Roles, Services, and Authentication	3
4. Finite State Model	2
5. Physical Security	2
6. Operational Environment	N/A
7. Cryptographic Key Management	2
8. EMI/EMC	3
9. Self-Tests	2
10. Design Assurance	3
11. Mitigation of Other Attacks	N/A
Overall Level	2

Table 1 - FIPS 140-2 Sections

2.4. Tested Modules

The modules which have been tested are listed in ***Table 2***. The Integral AES 256 Bit Crypto SSD Underlying PCB executes in a non-modifiable proprietary operational environment. Every module specified in the following table can contain either a PS3105 or PS3108 processor. Modules that have the same interfaces are visually indistinguishable from each other as they only differ in memory size.

Model	***Hardware Version***	***Memory Option***	***Visual Representation***
2.5” SATA II & III	INSSD32GS25MCR140-2(R)	32GB	See Figure 2
2.5” SATA II & III	INSSD64GS25MCR140-2(R)	64GB	
2.5” SATA II & III	INSSD128GS25MCR140-2(R)	128GB	
2.5” SATA II & III	INSSD256GS25MCR140-2(R)	256GB	
2.5” SATA II & III	INSSD512GS25MCR140-2(R)	512GB	
2.5” SATA II & III	INSSD1TS25MCR140-2(R)	1TB	
2.5” SATA III	INIS2564GCR140(R)	64GB	
2.5” SATA III	INIS25128GCR140(R)	128GB	
2.5” SATA III	INIS25256GCR140(R)	256GB	
2.5” SATA III	INIS25512GCR140(R)	512GB	
2.5” SATA III	INIS251TCR140(R)	1TB	
2.5” SATA III	INIS252TCR140(R)	2TB	
2.5” SATA III	INSSD64GS625M7CR140(R)	64GB	

Model	Hardware Version	Memory Option	Visual Representation
2.5” SATA III	INSSD128GS625M7CR140(R)	128GB	
2.5” SATA III	INSSD256GS625M7CR140(R)	256GB	
2.5” SATA III	INSSD512GS625M7CR140(R)	512GB	
2.5” SATA III	INSSD1TS625M7CR140(R)	1TB	
2.5” SATA III	INSSD2TS625M7CR140(R)	2TB	
1.8” SATA II & III	INSSD32GS18MCR140-2(R)	32GB	
1.8” SATA II & III	INSSD64GS18MCR140-2(R)	64GB	
1.8” SATA II & III	INSSD128GS18MCR140-2(R)	128GB	
1.8” SATA II & III	INSSD256GS18MCR140-2(R)	256GB	
1.8” SATA II & III	INSSD512GS18MCR140-2(R)	512GB	
1.8” SATA II & III	INSSD1TGS18MCR140-2(R)	1TB	See Figure 3
1.8” SATA III	INIS1864GCR140(R)	64GB	
1.8” SATA III	INIS18128GCR140(R)	128GB	
1.8” SATA III	INIS18256GCR140(R)	256GB	
1.8” SATA III	INIS18512GCR140(R)	512GB	
1.8” SATA III	INIS181TGCR140(R)	1TB	
1.8” SATA III	INIS182TGCR140(R)	2TB	
Half Slim SATA III	INISHS64GCR140(R)	64GB	
Half Slim SATA III	INISHS128GCR140(R)	128GB	
Half Slim SATA III	INISHS256GCR140(R)	256GB	See Figure 4
Half Slim SATA III	INISHS512GCR140(R)	512GB	
Half Slim SATA III	INISHS1TCR140(R)	1TB	
Half Slim SATA III	INISHS2TCR140(R)	2TB	
M.2 SATA 2260	INSSD128GM2M2260C140(R)	128GB	
M.2 SATA 2260	INSSD256GM2M2260C140(R)	256GB	
M.2 SATA 2260	INSSD512GM2M2260C140(R)	512GB	
M.2 SATA 2260	INSSD1TM2M2260C140(R)	1TB	
M.2 SATA 2260	INIM26064GCR140(R)	64GB	
M.2 SATA 2260	INIM260128GCR140(R)	128GB	
M.2 SATA 2260	INIM260256GCR140(R)	256GB	
M.2 SATA 2260	INIM260512GCR140(R)	512GB	
M.2 SATA 2260	INIM2601TCR140(R)	1TB	See Figure 5
M.2 SATA 2260	INIM2602TCR140(R)	2TB	
M.2 SATA 2280	INSSD64GM2M2280C140(R)	64GB	
M.2 SATA 2280	INSSD128GM2M2280C140(R)	128GB	
M.2 SATA 2280	INSSD256GM2M2280C140(R)	256GB	
M.2 SATA 2280	INSSD512GM2M2280C140(R)	512GB	
M.2 SATA 2280	INSSD1TGM2M2280C140(R)	1TB	
M.2 SATA 2280	INIM28064GCR140(R)	64GB	
M.2 SATA 2280	INIM280128GCR140(R)	128GB	

Model	Hardware Version	Memory Option	Visual Representation
M.2 SATA 2280	INIM280256GCR140(R)	256GB	
M.2 SATA 2280	INIM280512GCR140(R)	512GB	
M.2 SATA 2280	INIM2801TCR140(R)	1TB	
M.2 SATA 2280	INIM2802TCR140(R)	2TB	
mSATA	INSSD64GMSA6MCR140(R)	64GB	
mSATA	INSSD128GMSA6MCR140(R)	128GB	
mSATA	INSSD256GMSA6MCR140(R)	256GB	
mSATA	INSSD512GMSA6MCR140(R)	512GB	
mSATA	INSSD1TMSA6MCR140(R)	1TB	
mSATA	INIMSA64GCR140(R)	64GB	See Figure 6
mSATA	INIMSA128GCR140(R)	128GB	
mSATA	INIMSA256GCR140(R)	256GB	
mSATA	INIMSA512GCR140(R)	512GB	
mSATA	INIMSA1TCR140(R)	1TB	
mSATA	INIMSA2TCR140(R)	2TB	
M.2 SATA 2242	INIM24264GCR140(R)	64GB	
M.2 SATA 2242	INIM242128GCR140(R)	128GB	
M.2 SATA 2242	INIM242256GCR140(R)	256GB	See Figure 7
M.2 SATA 2242	INIM242512GCR140(R)	512GB	
M.2 SATA 2242	INIM2421TCR140(R)	1TB	
M.2 SATA 2242	INIM2422TCR140(R)	2TB	

Table 2 - Tested Modules

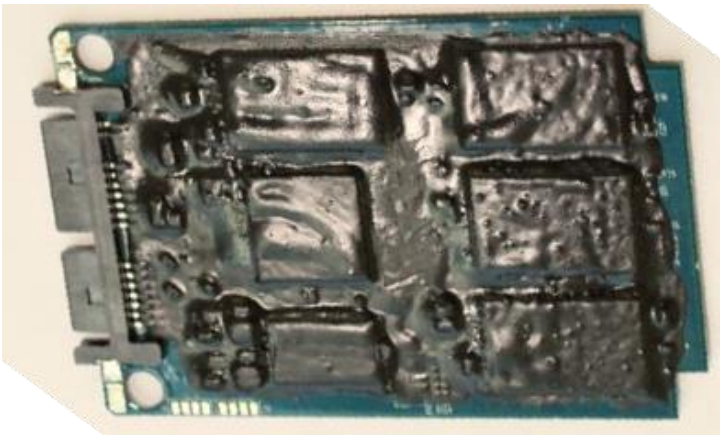

Figure 2 – 2.5" SATA Models

Figure 3 – 1.8" SATA Modules

Figure 4 – Half Slim SATA Models

Figure 5 – M.2 2260 & 2280 SATA Models

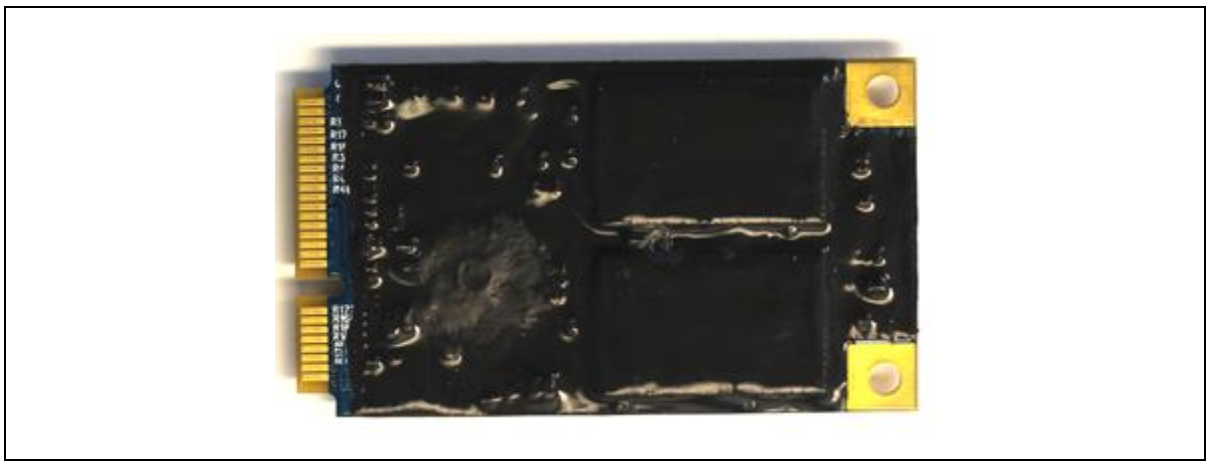

Figure 6 – mSATA Models

Figure 7 – M.2 2242 SATA Models

3. Approved Mode of Operation

3.1. FIPS Approved Mode

The modules only operate in the Approved mode of operation, meaning no configuration exists whereby the modules can operate in a non-Approved mode. The instructions to securely configure and initialize the modules into the Approved mode are as follows:

1. Install the Integral AES 256 Bit Crypto SSD into the host computer or laptop;
2. Install the Windows Operating System;
3. Run the SSDLock software;
4. Enter language;
5. Create a password 8-16 Characters long for the master;
6. Create a password 8-16 characters long for the user;
7. Choose how many login attempts allowed;
8. Re-start the Computer or Laptop; and
9. Enter the Password for the User or Master Account.

The module will confirm that the Approved mode has been entered by presenting the operator with the login prompt.

3.2. Crypto Officer and User Guidance

In order to ensure compliance with best security practices, the following rules ***shall*** be observed when operating the module in the Approved mode unless otherwise indicated:

- The Crypto Officer ***shall*** inspect the packaging after taking delivery of the module for any signs of tampering. The module ***shall*** be sent back if there is any evidence the module may have been tampered with during shipping.
- Usernames and passwords ***shall*** be uniquely assigned and not shared between operators.
- The Crypto-Officer ***shall*** periodically inspect the module as instructed in Section Physical Security of this document.
- The Crypto-Officer ***shall*** retain the correct password. If the password is incorrect after 20 attempts, all keys, CSPs and user data will be zeroized.
- It is ***recommended*** that Crypto Officers and users meet the maximum password length rather than the minimum password length when configuring passwords.

4. Module Ports & Interfaces

This section maps the FIPS 140-2 logical interfaces to the module's physical interface as follows:

- Data Input logical Interface maps to the physical SATA data cable interface of the module.
- Data Output logical interface maps to the physical SATA data cable interface of the module.
- Control Input logical interface maps to the physical SATA data cable interface of the module.
- Status output logical interface maps to the physical SATA data cable interface of the module.
- The module contains a power interface which maps to the physical SATA power cable interface of the module. This interface requires power from the host hardware platform.

***NOTE:** All four FIPS 140-2 logical interfaces map to the SATA interface of each module listed in Table 2.

5. Roles, Services & Authentication

The modules support the following two roles:

1) Crypto Officer role:
   This role is also referred to as the 'Master' role. This is the role assumed by an operator to perform cryptographic initialization, management functions, and cryptographic operations.

2) User role:
   This is the role assumed by an operator to perform general security services, including cryptographic operations.

The modules implement identity-based authentication comprised of a username and password combination. The Crypto Officer role and the User role are explicitly assumed by the operator by successfully authenticating to the module using the correct username and password combination.

5.1. Identification & Authentication

The authentication methods employed by the module are described here in **Table 3**. After 20 unsuccessful authentication attempts the module zeroizes all Keys, CSPs and data.

Role	Authentication (User name and Password combination)	Auth. Strength	Multi-Attempt in 60 sec. Strength
Crypto Officer (Master)	Passwords must meet each of the following requirements: • 8 to 16 characters in length • 1 upper case alphabetical character • 1 lower case alphabetical character • 1 numeric character • 1 special character	Probability of a random attempt succeeding is: 1: 6 041 130 045 251 584 (52 bits of strength)	Probability of random attempts during a one minute period succeeding are: 1:302 056 502 262 579 (48 bits of strength)
User	Passwords must meet each of the following requirements: • 8 to 16 characters in length • 1 upper case alphabetical character • 1 lower case alphabetical character • 1 numeric character • 1 special character	Probability of a random attempt succeeding is: 1: 6 041 130 045 251 584 (52 bits of strength)	Probability of random attempts during a one minute period succeeding are: 1:302 056 502 262 579 (48 bits of strength)

Table 3 - Roles & Authentication Methods

5.2. Roles & Services

The services that are available to operators are listed in **Table 4**. The table specifies the authorized services by the operator roles and identifies the Cryptographic Keys and CSPs associated with the services. The modes of access are also identified per the explanation.

Legend

N/A – The service is not associated with a key or CSP
DEK – Data Encryption Key
Password – Operator Password
Seed – Random seed consumed by NIST SP 800-90A DRBG

R - The item is **read** or referenced by the service.
W - The item is **written** or updated by the service.
E - The item is **executed** by the service. (The item is used as part of a cryptographic function.)

Service	Roles	Keys & CSPs	Algorithm	RWE
Self-Test	Crypto-Officer & User	N/A	N/A	E
Authenticate	Crypto-Officer & User	Password	N/A	W, E
Create & Change Password	Crypto-Officer	Password	N/A	W, E
Password Reset	Crypto-Officer	Password	N/A	W, E
Delete User	Crypto-Officer	Password	N/A	
Lock	Crypto-Officer User	N/A	N/A	E
Show Status	Crypto-Officer User	N/A	N/A	R
Key Generation	Crypto-Officer User	DEK, DRBG V, DRBG Key	AES DRBG	W, E
Encrypt/Decrypt	Crypto-Officer User	DEK	AES	W, E
Hash	Crypto-Officer User	N/A	N/A	W
Reset (Zeroize)	Crypto-Officer User	DEK, DRBG V, DRBG Key, Password	AES DRBG	W, E
Logout	Crypto-Officer User	N/A	N/A	E

Table 4 - Roles & Services

6. Physical Security

6.1. Physical Security Mechanisms

The modules are contained within a removable metal chassis, however the cryptographic boundary for the modules is defined as the outer surface of the epoxy resin which covers the module's PCB board, electronic components, and circuitry. The modules' physical boundaries do not include the steel chassis in which the modules are shipped. The modules are comprised of off-the-shelf production grade components that include standard passivation. The modules are opaque within the visible spectrum and do not have any removable covers, openings, or doors. In the event that the hard coating protecting the PCB is breached to the depth of the underlying circuitry, the module will cease to function completely. The module should be replaced immediately if any type of damage is witnessed.

It is the responsibility of the Crypto-Officer to periodically inspect the module for tamper evidence. This requires the removal of the outer metal chassis to be able to inspect the epoxy resin to ensure that it has not been breached and does not show and signs of attempted tampering.

To inspect the module, the Crypto Officer shall perform the following at a frequency of at least once every six months:

- Remove the (4) standard Phillips screws from the metal casing in which the module ships;
- Remove the module from the metal chassis; and
- Closely inspect the epoxy resin coating for any evidence of tamper (evidence includes chipping, and/or scraping, and/or drilling of the epoxy resin coating).

If the Crypto Officer discovers tamper evidence during a physical inspection of the module the following action ***shall*** be taken:

- Zeroize all keys and CSPs; and
- Return the module to Integral Memory. The module must be replaced.

****The module hardness testing was only performed at room temperature and no assurance is provided for Level 3 hardness conformance at any other temperature.***

7. Operational Environment

The Integral AES 256 Bit Crypto SSD Underlying PCBs S5FDM018 firmware provides a limited a proprietary, non-modifiable operational environment.

8. Key Management

8.1. Cryptographic Keys and CSPs

The module does not allow for the input or output of any keys, key components, or CSPs. The table below outlines the cryptographic keys, key components, and CSPs used by the modules.

Key/CSP	Use	Generation	Zeroization	Storage
Data Encryption Key (AES)	Used for data encryption and data decryption	Generated internally	Reset command or exceeding password attempt threshold	Stored as plaintext in Flash memory
Password	Operator Authentication (Role assumption)	N/A	Reset command or exceeding password attempt threshold	Stored hashed in Flash memory
Seed Data for SP 800-90A DRBG	DRBG random number generation	Generated internally	Reset command or exceeding password attempt threshold	Stored plaintext in volatile RAM
HMAC Key	DRBG random number generation	Generated internally	Reset command or exceeding password attempt threshold	Stored plaintext in volatile RAM

Table 5 – Cryptographic Keys, Key Components, and CSPs

9. Cryptographic Algorithms

9.1. Cryptographic Algorithms

Table 6 specifies all of the algorithms used by the module.

Algorithm	CAVP Algorithm Certificate	Implemented In
Symmetric Key		
Advanced Encryption Standard (AES) 256-bit in CBC mode	2175	Hardware
Advanced Encryption Standard (AES) 128/256-bit in XTS mode	2175	Hardware
Message Authentication		
HMAC-SHA-256, 512	1335	Firmware
Secure Hash Standard		
SHA-256, 512	1887	Hardware
Random Number Generator		
NIST SP 800-90A HMAC_DRBG	254	Firmware
NDRNG (non-approved but allowed)	NA	Hardware

Table 6 - Algorithm Certificates

10. Self-Tests

10.1. Power Up Self-Tests

The modules perform the following power-up self-tests after power has been applied to the module. Once power has been applied the power-up self-tests will execute automatically without any intervention from the operator:

- Firmware Integrity Test using SHA-512
- AES Known Answer Test (encrypt)
- AES Known Answer Test (decrypt)
- SHA-256, SHA-512 Known Answer Test
- DRBG Known Answer Test
- HMAC SHA-256 and 512 Known Answer Test

10.2. Conditional Tests

The modules perform the following conditional tests as required:

- Continuous RNG test for the SP 800-90A DRBG
- Continuous RNG test on the NDRNG

10.3. Self-Test Failure

If *any* self-test fails the module will transition into the error state and an error message will be output via the status output interface (message will be displayed on-screen). While in the error state the modules' data input, data output, and control input interfaces are disabled and as a result data output is inhibited while the module is in the error state. Additionally, all cryptographic operations are prohibited from taking place while the module is in the error state. The operator can attempt to clear the error by power cycling the host PC with the module connected. Should the module encounter another error during the subsequent power-up self-tests then the error is considered to be unrecoverable. The module should be replaced in this circumstance.

10.4. On-Demand Self-Tests

In order to execute the power-up self-tests on demand, the operator can reboot the host PC which the module is connected to. Self-Tests execute without operator intervention when the module receives power.

11. Design Assurance

11.1. Secure Delivery

When the module is shipped to the customer, a bonded courier is used. The Crypto-Officer is advised to check the packaging when accepting delivery of the module and to send it back if there is any evidence of tampering.

11.2. Configuration Management

Each version of each configuration item for both the cryptographic module and associated documentation is assigned and labeled with a unique identification number by Integral Memory.

12. Mitigation of Other Attacks

The modules do not claim mitigation of other attacks.